UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,397	10/16/2003	Graeme John Proudler	82170341	1309

22879 7590 10/27/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
MORAN, RANDAL D	
ART UNIT	**PAPER NUMBER**
2435	

NOTIFICATION DATE	DELIVERY MODE
10/27/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte GRAEME JOHN PROUDLER

Appeal 2009-012007
Application 10/688,397
Technology Center 2400

Before ALLEN R. MACDONALD, JASON V. MORGAN, and
ERIC B. CHEN, *Administrative Patent Judges.*

CHEN, *Administrative Patent Judge.*

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the final rejection of claims 35-42, 44 and 46-49. Claims 1-34, 43 and 45 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

Appellant's invention relates to an access-control arrangement for handling a tree-structured hierarchy such as a key hierarchy. (Spec. Abstract.)

Claim 35 is exemplary, with disputed limitations in italics:

35. A computing platform comprising:

a secure key-handling unit arranged to store a storage root key that forms the root node of a tree-structured node hierarchy the non-leaf nodes of which, other than the root node, each comprise, in encrypted form, a key used to encrypt the or each of its child nodes, and

insecure storage for storing the hierarchy nodes other than the root node;

the key-handling unit comprising:

a memory for storing a current decryption-root key;

a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key; and

a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

Claims 35-42, 44 and 46-49 stand rejected under 35 U.S.C. § 103(a) as being obvious over Challener (U.S. Patent Application Publication No. 2002/0059286) and Ishiguro (U.S. Patent No. 5,796,839).

We are not persuaded by Appellant's arguments (App. Br. 5-6; *see also* Reply Br. 2-3) that the combination of Challener and Ishiguro would

not have rendered obvious independent claim 35, including the disputed limitation "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key."

The Examiner found that the trusted platform module chip (TPM) of Challener including a storage root key 101 corresponds to this disputed limitation. (Ans. 3, 7-8.) In particular, the Examiner found that "Challener explicitly discloses a decrypted access arrangement (i.e. the storage root key being used to decrypt all leaf nodes below it)." (Ans. 8; Challener, ¶ [0021].) We agree with the Examiner.

Challener describes a typical design of a trusted platform module chip (TPM) that includes "a storage root key 101, which would have a platform migratable key 102, which would also have a user key 103, which would then have signing keys 104-106." (¶ [0021]; fig. 1.) The storage root key 101 is used to store other keys (i.e., children keys), such that the chip decrypts these other keys. (¶ [0021].) In other words, Challener teaches the limitation "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key."

Appellant argues that:

> [T]he only "current decryption-root key" disclosed in Challener is the storage root key itself and all the hierarchy nodes are decryptable by a chain of decryption rooted in the storage root key – therefore there is no concept of less than the whole hierarchy being decryptable in Challener and therefore no concept of an arrangement restricting decrypted access to a subset of the nodes of the hierarchy.

(App. Br. 6.)

However, this argument is not commensurate in scope with claim 35 because the claim does not require that only a subset of the whole hierarchy nodes be decryptable.

Therefore, we agree with the Examiner that the combination of Challener and Ishiguro would have rendered obvious independent claim 35, including the disputed limitation "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key."

We are also not persuaded by Appellant's arguments (App. Br. 8-11; *see also* Reply Br. 4) that the combination of Challener and Ishiguro would not have rendered obvious independent claim 35, including the disputed limitation "a current-decryption-root setting arrangement."

The Examiner acknowledged that Challener does not disclose the second disputed limitation and therefore cited Ishiguro. (Ans. 3-4.) In particular, the Examiner found that the disclosure in Ishiguro of selecting an encryption key of a proper generation from hierarchized keys corresponds to this disputed limitation. (Ans. 9.) The Examiner concluded that "it would have been obvious . . . to modify the teachings of Challener by the current decryption-root arrangement as taught by Ishiguro to provide a decoding apparatus in which encryption keys can be managed with ease." (Ans. 4.) We agree with the Examiner.

As discussed previously, Challener describes a trusted platform module chip (TPM). (¶ [0021].) Ishiguro relates to the encryption of software or data (col. 1, ll. 8-14) (e.g., encrypted software or data recorded on a digital video disk (col. 1, ll. 24-29)). Ishiguro describes that each time an encryption key is updated, the previous encryption key is retained such

that "the hardware and the software both face problems of managing the retained encryption keys" (col. 1, ll. 59-67) and thus, "it is an object of the present invention to provide an encryption method . . . in which encryption keys can be managed with ease by hierarchizing encryption keys" (col. 2, ll. 6-11). Ishiguro describes a master key read out from a memory 12 of an IC chip 11 and set to a selection key (k) that is supplied to a decoding circuit 14, such that the selection key (k) is expressed as an encryption key. (Col. 6, ll. 29-34.) In other words, Ishiguro teaches the limitation "a current-decryption-root setting arrangement."[1]

A person of ordinary skill in the art at the time of the invention would have recognized that incorporating the master key and the selection key (k) of Ishiguro, with the trusted platform module chip (TPM) of Challener would improve Challener by facilitating the management of encryption keys. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 417 (2007). Thus, we agree with the Examiner (Ans. 4) that modifying Challener to include the master key and the selection key (k) of Ishiguro would have been obvious.

Appellant argues that "Ishiguru has no concept of an arrangement for restricting access to only some of the hierarchy nodes because Ishiguru always starts with the available key that is highest up the hierarchy." (App. Br. 9.) Again, this argument is not commensurate in scope with claim 35 because the claim does not require restricting access to only some of the hierarchy nodes.

---

[1] Appellant also admits that "we agree that Ishiguro discloses the current-decryption-root setting arrangement" and "Ishiguro must also implicitly have a memory for storing the key acting as the current decryption root key." (App. Br. 8.)

Appellant also argues that "[t]he Examiner has provided no articulated reasoning with some rational underpinning to support his legal conclusion of obviousness" because "the required security properties of the Challener TPM make it highly undesirable that the keys of its key hierarchy are cryptographically related to each other as in Ishiguro." (App. Br. 11; *see also* Reply Br. 4.) However, as discussed previously, the combination of Challener and Ishiguro is based on the improvement of a similar device in the same way as in the prior art. Furthermore, Appellant has not provided any persuasive evidence to support the argument that the TPM of Challener and the encryption keys of Ishiguro are incompatible. Arguments of counsel cannot take the place of factually supported objective evidence. *See, e.g.*, *In re Huang*, 100 F.3d 135, 139-140 (Fed. Cir. 1996).

Therefore, we agree with the Examiner that the combination of Challener and Ishiguro would have rendered obvious independent claim 35, including the disputed limitation "a current-decryption-root setting arrangement."

Accordingly, we sustain the rejection of independent claim 35 under 35 U.S.C. § 103(a). Claims 36-42, 44 and 46-49 depend from independent claim 35 and Appellant has not presented any substantive arguments with respect to these claims. Therefore, we sustain the rejection of claims 36-42, 44 and 46-49 under 35 U.S.C. § 103(a) for the same reasons discussed with respect to independent claim 35.

DECISION

The Examiner's decision to reject claims 35-42, 44 and 46-49 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

tj